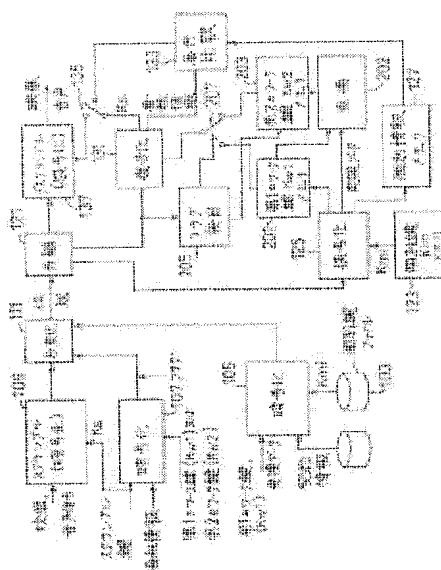


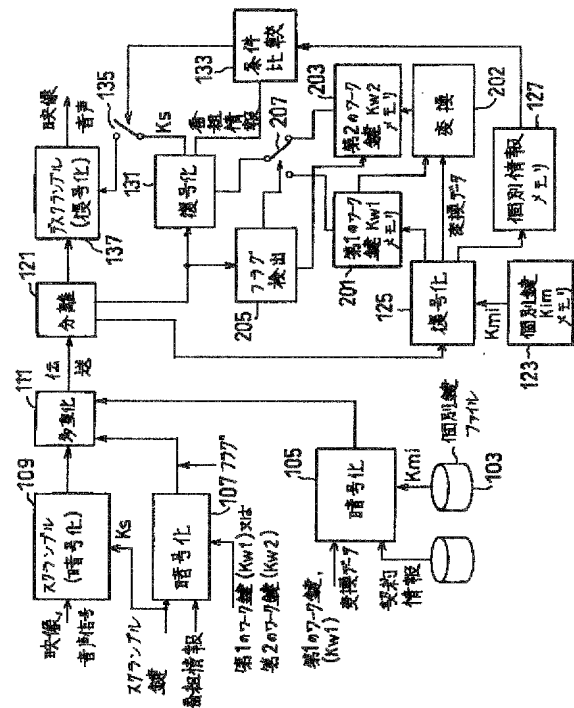
PAY BROADCAST SYSTEM AND ITS ENCODER AND DECODER**Publication number:** JP9307872 (A)**Publication date:** 1997-11-28**Inventor(s):** OI SHINICHI**Applicant(s):** TOKYO SHIBAURA ELECTRIC CO**Classification:**- international: **H04N7/167; G06F21/24; H04H20/00; H04H60/15; H04H60/23; H04L9/08; H04N7/167; G06F21/00; H04H1/00; H04L9/08; (IPC1-7): H04N7/167; H04H1/00**

- European:

Application number: JP19960117369 19960513**Priority number(s):** JP19960117369 19960513**Abstract of JP 9307872 (A)****PROBLEM TO BE SOLVED:** To reduce number of transmission times for individual information.**SOLUTION:** A ciphering circuit 105 ciphers a 1st substantial work key and conversion data. As a key of a ciphering circuit 107, the 1st work key or a 2nd work key obtained by converting the 1st work key with conversion data is used. A decoding circuit 125 recovers the 1st work key and the conversion data. A conversion circuit 202 converts the 1st work key by the conversion data to generate a 2nd work key. A decoding circuit 131 uses the 1st or 23rd work key corresponding to the ciphered key of the ciphering circuit 107.

Data supplied from the esp@cenet database — Worldwide

(11)特許出願公開番号



1

【特許請求の範囲】

【請求項 1】 少なくとも 3 層の暗号構造を有する有料放送において、

第 3 の層の第 1 の鍵により個別情報、第 2 層の第 2 の鍵、前記第 2 の鍵の変換データを暗号化する第 1 の暗号化手段と、

前記第 2 の鍵または前記第 2 の鍵を前記変換データにより変換して得られた第 3 の鍵により番組情報とスクランブル鍵を暗号化する第 2 の暗号化手段と、

前記第 1 の復号化手段の出力を前記第 1 の鍵により復号し、前記個別情報、前記第 2 の鍵、前記変換データを再生する第 1 の復号化手段と、

前記第 2 の鍵を記憶する第 1 の記憶手段と、

前記第 1 の記憶手段からの前記第 2 の鍵を前記変換データにより変換して前記第 3 の鍵を生成する変換手段と、前記変換手段からの前記第 3 の鍵を記憶する第 2 の記憶手段と、

前記第 1 の記憶手段からの前記第 2 の鍵または前記第 2 の記憶手段からの前記第 3 の鍵により、前記第 2 の暗号化手段の出力を復号し、前記番組情報と前記スクランブル鍵を再生する第 2 の復号手段と、

を具備したことを特徴とする有料放送方式。

【請求項 2】 前記変換データは、前記第 2 の鍵の各ビットの順序の入れ替え方のデータであることを特徴とする請求項 1 記載の有料放送方式。

【請求項 3】 前記変換データは、前記第 2 の鍵のデータの回転方向と回転量を示すデータであることを特徴とする請求項 1 記載の有料放送方式。

【請求項 4】 前記変換データは、前記第 2 の鍵のビット順序の反転を指示するデータであることを特徴とする請求項 1 記載の有料放送方式。

【請求項 5】 前記変換データは、前記第 2 の鍵への加算データであることを特徴とする請求項 1 記載の有料放送方式。

【請求項 6】 少なくとも 3 層の暗号構造を有するエンコーダにおいて、

第 3 の層の第 1 の鍵により個別情報、第 2 層の第 2 の鍵、前記第 2 の鍵の変換データを暗号化する第 1 の暗号化手段と、

前記第 2 の鍵または前記第 2 の鍵を前記変換データにより変換して得られた第 3 の鍵により番組情報とスクランブル鍵を暗号化する第 2 の暗号化手段と、

を具備したことを特徴とするエンコーダ。

【請求項 7】 前記変換データは、前記第 2 の鍵の各ビットの順序の入れ替え方のデータであることを特徴とする請求項 6 記載のエンコーダ。

【請求項 8】 前記変換データは、前記第 2 の鍵のデータの回転方向と回転量を示すデータであることを特徴とする請求項 6 記載のエンコーダ。

【請求項 9】 前記変換データは、前記第 2 の鍵のビッ

2

ト順序の反転を指示するデータであることを特徴とする請求項 6 記載のエンコーダ。

【請求項 10】 前記変換データは、前記第 2 の鍵への加算データであることを特徴とする請求項 6 記載のエンコーダ。

【請求項 11】 少なくとも 3 層の暗号構造を有し、第 3 の層の第 1 の鍵により個別情報、第 2 層の第 2 の鍵、前記第 2 の鍵の変換データを暗号化する第 1 の暗号化手段と、

前記第 2 の鍵または前記第 2 の鍵を前記変換データにより変換して得られた第 3 の鍵により番組情報とスクランブル鍵を暗号化する第 2 の暗号化手段と、

を具備したエンコーダから伝送されてくる放送を受信するデコーダにおいて、

前記第 1 の復号化手段の出力を前記第 1 の鍵により復号し、前記個別情報、前記第 2 の鍵、前記変換データを再生する第 1 の復号化手段と、

前記第 2 の鍵を記憶する第 1 の記憶手段と、

前記第 1 の記憶手段からの前記第 2 の鍵を前記変換データにより変換して前記第 3 の鍵を生成する変換手段と、

前記変換手段からの前記第 3 の鍵を記憶する第 2 の記憶手段と、

前記第 1 の記憶手段からの前記第 2 の鍵または前記第 2 の記憶手段からの前記第 3 の鍵により、前記第 2 の暗号化手段の出力を復号し、前記番組情報と前記スクランブル鍵を再生する第 2 の復号手段と、

を具備したことを特徴とするデコーダ。

【請求項 12】 前記変換データは、前記第 2 の鍵の各ビットの順序の入れ替え方のデータであることを特徴とする請求項 11 記載のデコーダ。

【請求項 13】 前記変換データは、前記第 2 の鍵のデータの回転方向と回転量を示すデータであることを特徴とする請求項 11 記載のデコーダ。

【請求項 14】 前記変換データは、前記第 2 の鍵のビット順序の反転を指示するデータであることを特徴とする請求項 11 記載のデコーダ。

【請求項 15】 前記変換データは、前記第 2 の鍵への加算データであることを特徴とする請求項 11 記載のデコーダ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、有料放送方式並びにそのエンコーダとデコーダに関する。

【0002】

【従来の技術】 有料放送では、契約した者のみが放送を享受できるように、映像及び音声信号にスクランブルを施し放送を行っている。

【0003】 このスクランブルを解除する処理は、大きく分けて 2 つある。1 つは、映像及び音声信号にかけられたスクランブルを解除し、元の信号に戻す処理であ

る。もう1つは、そのデスクランブルがスクランブルを解除しても良いか否かの判断を行う処理つまり放送局との契約状態を条件比較して判断し、デスクランブル処理のON/OFFを管理する処理の2つである。

【0004】この契約管理処理では、放送局から送られてくる情報を使用するが、その情報には暗号がかけられており、契約した者のデコーダのみが情報を取り込めるようになっている。

【0005】図8に従来の有料放送システムの構成を示す。図示したように暗号化するデータは、階層構造になっている。

【0006】暗号化回路105には、暗号化されるものとして、放送局から各デコーダへの個別の契約情報（以下、個別情報という）とワーク鍵Kwが供給されている。前記個別情報は、契約した者のデコーダが視聴できるようにするための情報である。暗号化回路105には、また個別鍵ファイル103から個別鍵Kmi（iは、個別鍵がデコーダごとに異なることを示すためにつけた）が供給されている。暗号化回路105は、個別鍵Kmiにより個別情報とワーク鍵Kwを暗号化する。

【0007】このため、その個別鍵を有しないデコーダでは、その暗号化されている情報を取り込むことができず、他人の情報を只見するような不正ができないようになっている。ただし、当然のことながら個別鍵は個々に異なるため、例えば10万台のデコーダを制御するためには、この個別情報を10万個送出する必要があるというように、個々のデコーダに対し情報を送る必要があり、管理するデコーダ数が増えると送るデータ量も多くなり大変である。

【0008】また、ワーク鍵Kwは、後述する番組情報を不正に利用されないように暗号化するための鍵である。暗号方式自体の解析がしにくいように、ワーク鍵Kwは定期的に変更することが必要であるとされている。

【0009】これは、例えば暗号化された番組情報とその復号結果の一部である後述するスクランブル鍵Ksとの関係から、ワーク鍵Kwや暗号方式そのものの解析をされる危険性があるので、その危険を低くするために、ワーク鍵Kwを変更するという考えによっている。

【0010】このため、例えば月に1度とかあるいは年に1度というタイミングでワーク鍵Kwを更新するよう

に、放送局からデコーダに対してワーク鍵Kwを含む個別情報を与えるようになっている。

【0011】暗号化回路107には、暗号化されるものとして、各デコーダに共通に与える番組に関する情報（以下、番組情報という）とスクランブル鍵Ksが供給される。暗号化回路107は、ワーク鍵Kwによって番組情報とスクランブル鍵Ksを暗号化する。

【0012】スクランブル回路109には、暗号化されるものとして映像、音声信号が供給される。スクランブル回路109は、スクランブル鍵Ksによって映像、音

声信号を暗号化する。

【0013】多重化回路111は、暗号化回路105、暗号化回路107、スクランブル回路109からの信号を多重する。多重化された信号は、デコーダ側に伝送される。

【0014】分離回路121は、入力を分離し、暗号化回路105の出力信号を復号化回路125に、暗号化回路107の出力信号を復号化回路131に、スクランブル回路109の出力信号をデスクランブル回路137に供給する。

【0015】復号化回路125は、個別鍵Kmiメモリ123からの個別鍵Kmiにより暗号化回路105の出力信号を復号し、個別情報とワーク鍵Kwを再生する。個別情報は、個別情報メモリ127に記憶され、ワーク鍵Kwは、ワーク鍵Kwメモリ129に記憶される。

【0016】復号化回路131は、ワーク鍵Kwメモリ129からのワーク鍵Kwにより暗号化回路107の出力信号を復号し、番組情報とスクランブル鍵Ksを再生する。スクランブル鍵Ksは、スイッチ135に供給される。

【0017】条件比較回路133は、個別情報メモリ127からの個別情報と復号化回路131からの番組情報を比較し、視聴可能であればスイッチ135をONにする。その結果、スクランブル鍵Ksが、デスクランブル回路137に供給される。

【0018】デスクランブル回路137は、スクランブル鍵Ksによりスクランブル回路109の出力信号を復号し、映像、音声信号を再生する。

【0019】

【発明が解決しようとする課題】上述したように、個別鍵Kmiはデコーダごとに異なるため、ワーク鍵Kwを更新し個々のデコーダへ与えるためには台数分の個別情報を送出しなければならない。しかし、デコーダ数が増えてくると、個別情報を送付するデータ量が膨大になり、データを送付するチャンネル容量を大きくするかあるいは全てのデコーダを制御するまでに必要な時間を長くとするなどの措置をとる必要があった。

【0020】そこで本発明は、ワーク鍵を更新するたびに個別情報を送る必要の無い有料放送方式並びにそのエンコーダとデコーダを提供することを目的とする。

【0021】

【課題を解決するための手段】

（有料放送方式）少なくとも3層の暗号構造を有する有料放送において、第3の層の第1の鍵により個別情報、第2層の第2の鍵、前記第2の鍵の変換データを暗号化する第1の暗号化手段と、前記第2の鍵または前記第2の鍵を前記変換データにより変換して得られた第3の鍵により番組情報とスクランブル鍵を暗号化する第2の暗号化手段と、前記第1の復号化手段の出力を前記第1の鍵により復号し、前記個別情報、前記第2の鍵、前記変

換データを再生する第1の復号化手段と、前記第2の鍵を記憶する第1の記憶手段と、前記第1の記憶手段からの前記第2の鍵を前記変換データにより変換して前記第3の鍵を生成する変換手段と、前記変換手段からの前記第3の鍵を記憶する第2の記憶手段と、前記第1の記憶手段からの前記第2の鍵または前記第2の記憶手段からの前記第3の鍵により、前記第2の暗号化手段の出力を復号し、前記番組情報と前記スクランブル鍵を再生する第2の復号手段と、を具備したことを特徴とする。

【0022】(エンコーダ) 少なくとも3層の暗号構造を有するエンコーダにおいて、第3の層の第1の鍵により個別情報、第2層の第2の鍵、前記第2の鍵の変換データを暗号化する第1の暗号化手段と、前記第2の鍵または前記第2の鍵を前記変換データにより変換して得られた第3の鍵により番組情報とスクランブル鍵を暗号化する第2の暗号化手段と、を具備したことを特徴とする。

【0023】(デコーダ) 少なくとも3層の暗号構造を有し、第3の層の第1の鍵により個別情報、第2層の第2の鍵、前記第2の鍵の変換データを暗号化する第1の暗号化手段と、前記第2の鍵または前記第2の鍵を前記変換データにより変換して得られた第3の鍵により番組情報とスクランブル鍵を暗号化する第2の暗号化手段と、を具備したエンコーダから伝送されてくる放送を受信するデコーダにおいて、前記第1の復号化手段の出力を前記第1の鍵により復号し、前記個別情報、前記第2の鍵、前記変換データを再生する第1の復号化手段と、前記第2の鍵を記憶する第1の記憶手段と、前記第1の記憶手段からの前記第2の鍵を前記変換データにより変換して前記第3の鍵を生成する変換手段と、前記変換手段からの前記第3の鍵を記憶する第2の記憶手段と、前記第1の記憶手段からの前記第2の鍵または前記第2の記憶手段からの前記第3の鍵により、前記第2の暗号化手段の出力を復号し、前記番組情報と前記スクランブル鍵を再生する第2の復号手段と、を具備したことを特徴とする。

【0024】

【発明の実施の形態】図1に、本発明の有料放送方式の実施の形態の構成を示す。従来例と同じ動作をする回路については、同一参照番号を付し説明は省略する。

【0025】暗号化回路105には、個別情報(契約情報)、本来のワーク鍵である第1のワーク鍵Kw1とこの第1のワーク鍵Kw1を変換する変換データが供給される。前記変換データは、将来の第1のワーク鍵Kw1の変換を先取りするためのものである。暗号化回路105は、個別鍵Kmiにより個別情報、第1のワーク鍵、変換データを暗号化する。この暗号化されたデータ列を、図2に示す。

【0026】暗号化回路107に、スクランブル鍵Ksと番組情報が供給される。暗号化回路107は、スクラ

ンブル鍵Ksと番組情報を、第1のワーク鍵Kw1又は第2のワーク鍵Kw2により暗号化する。

【0027】第2のワーク鍵Kw2は、第1のワーク鍵Kw1を前記変換データで変換したものである。前記変換データの例とこの変換データによって生成された第2のワーク鍵Kw2の例を以下に説明する。

【0028】前記変換データの第1の例は、第1のワーク鍵Kw1の各ビットの順序の入れ替え方のデータである。この場合の変換例を、図4に示す。前記変換データの第2の例は、第1のワーク鍵Kw1のデータの回転方向と回転量を示すデータである。例えば、右まわりに2ビット分回転させる。この場合の変換例を、図5に示す。前記変換データの第3の例は、第1のワーク鍵Kw1のビット順序の反転を指示するデータである。この場合の変換例を、図6に示す。前記変換データの第4の例は、第1のワーク鍵Kw1の各ビットに加算を指示し、その加算するデータである。この場合の変換例を、図7に示す。尚、暗号化回路105でおくる変換データは、一種類に限らず、複数送ることも考えられる。

【0029】暗号化回路107の出力において、フラグが挿入される。フラグは、暗号化回路107において、どのワーク鍵を使用したかのデータと変換データの種類のデータである。

【0030】フラグを含む暗号化された番組情報、スクランブル鍵Ksのデータ列を、図3に示す。

【0031】復号化回路125は、個別鍵Kmiにより復号化を行い、個別情報、第1のワーク鍵Kw1、前記変換データを出力する。第1のワーク鍵Kw1は、第1のワーク鍵Kw1メモリ201に供給される。前記変換データは、変換回路202に供給される。変換回路202には、また第1のワーク鍵Kw1メモリ201から第1のワーク鍵Kw1が供給される。変換回路202は、上述したように前記変換データにより第1のワーク鍵Kw1を変換して、第2のワーク鍵Kw2を生成し、第2のワーク鍵Kw2メモリ203に供給する。各メモリ201、203からの第1と第2のワーク鍵Kw1とKw2が、スイッチ207に供給されている。

【0032】フラグ検出回路205は、フラグを検出し、暗号化回路107で使用したワーク鍵がどちらであるかを検出する。フラグ検出回路205は、第1のワーク鍵Kw1が使用された場合は、スイッチ207を第1のワーク鍵Kw1メモリ201側に倒し、第2のワーク鍵Kw2が使用された場合は、スイッチ207を第2のワーク鍵Kw2メモリ203側に倒す。フラグ検出回路205は、またどの変換データが使用されたかを検出し、第2のワーク鍵Kw2メモリから読み出す第2のワーク鍵Kw2の種類を選択する。

【0033】復号化回路131は、スイッチ207で選択されたワーク鍵により復号して、番組情報とスクランブル鍵Ksを出力する。

10

20

30

40

50

【0034】変換データとしては、複数の変換方法を組み合わせるものであっても良い。例えば、図4に示す変換をした後、図5に示す変換をしても良い。

【0035】変換データが一種類の場合、エンコーダ側でのフラグの挿入をやめると共に、フラグ検出回路205を省略する。この場合、復号化回路131は、第1と第2のワーク鍵Kw1とKw2を順次選択し合致するものを使用する。

【0036】また、グループ個別情報では、そのグループに含まれるデコーダに対するワーク鍵だけでなく、契約情報（グループ個別情報）も与えることになるため、ワーク鍵を更新させたくないデコーダを除いて契約情報を与えることができず不便であったが、本発明では契約情報に関しては、既にデコーダに蓄積されているものをそのまま使用するのでそのような不便がなく、ワーク鍵を変更できる。

【0037】

【発明の効果】上述したように、本発明では個別情報に本来の第1のワーク鍵Kw1を変換するデータをあらかじめ1つ以上入れておき、番組情報の復号時に、第1のワーク鍵Kw1を前記変換データで変換し使用するので、ワーク鍵を変更するためだけに個別情報を送らなくても良く、伝送チャンネルの有効利用をはかることができる。

【図面の簡単な説明】

【図1】本発明の有料放送システムの実施の形態の構成を示す図である。

【図2】暗号化された個別情報のデータ列を示す図である。

【図3】暗号化された番組情報、スクランブル鍵Ksのデータ列を示す図である。

【図4】本来の第1のワーク鍵Kw1の変換例を示す図である。

【図5】本来の第1のワーク鍵Kw1の変換例を示す図である。

【図6】本来の第1のワーク鍵Kw1の変換例を示す図である。

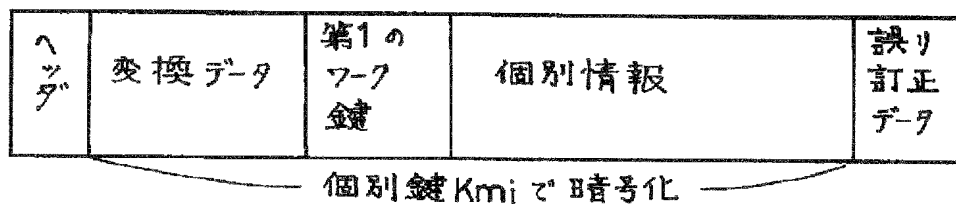
【図7】本来の第1のワーク鍵Kw1の変換例を示す図である。

【図8】従来の有料放送方式の構成を示す図である。

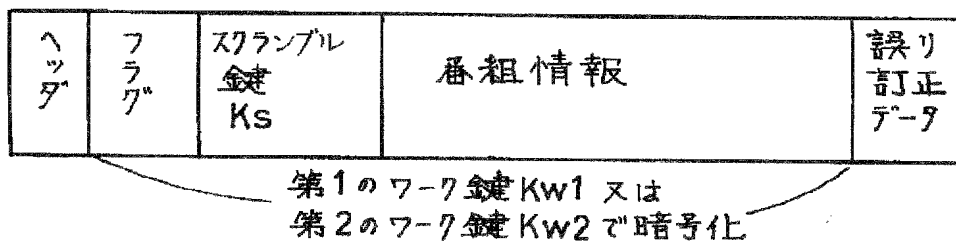
【符号の説明】

103・・・個別鍵ファイル、105、107・・・暗号化回路、109・・・スクランブル回路、111・・・多重化回路、121・・・分離回路、123・・・個別鍵Kmiメモリ、125・・・復号化回路、127・・・個別情報メモリ、131・・・復号化回路、133・・・条件比較回路、135・・・スイッチ、137・・・デスクランブル回路、201・・・第1のワーク鍵Kw1メモリ、202・・・変換回路、203・・・第2のワーク鍵Kw2メモリ、207・・・スイッチ。

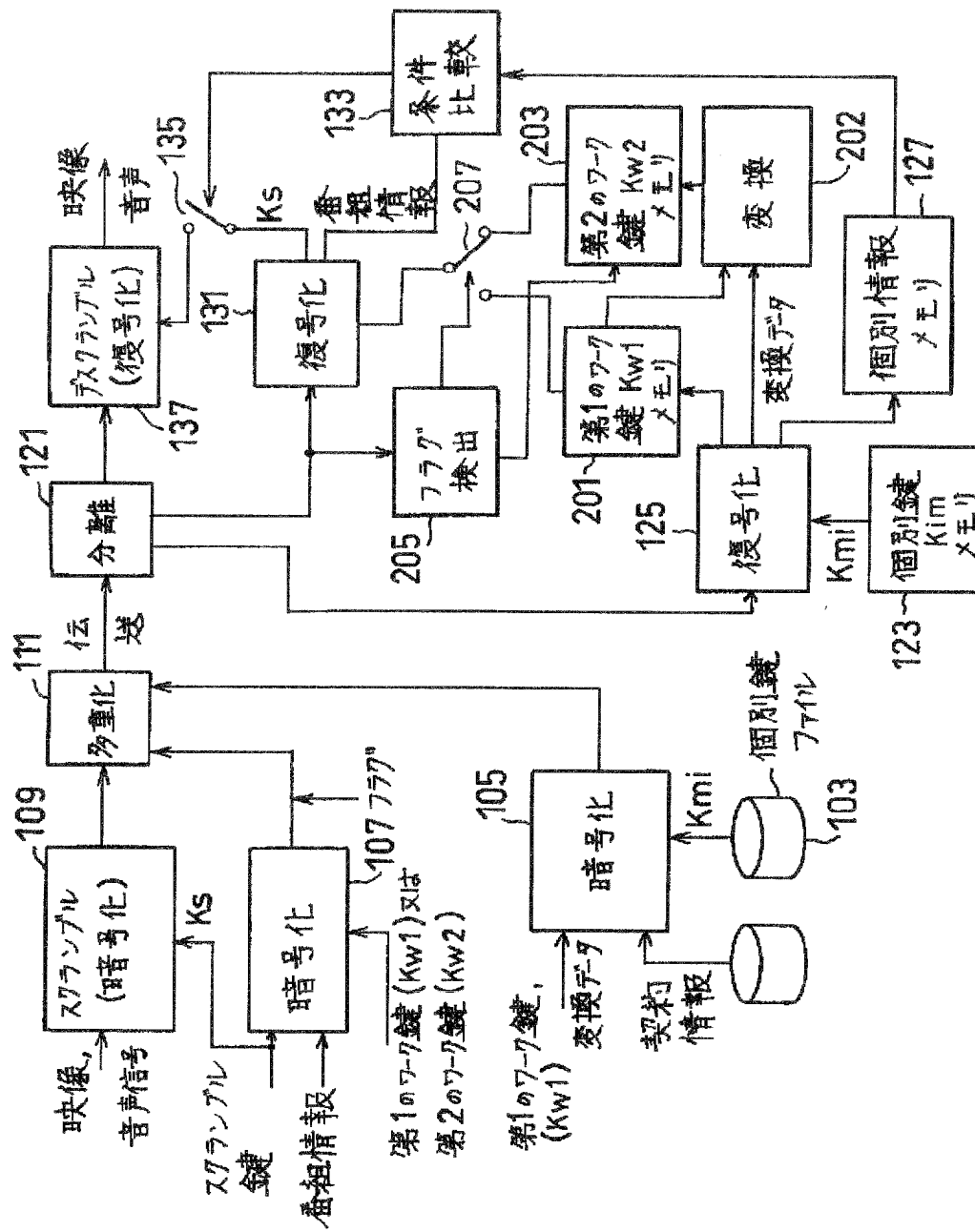
【図2】



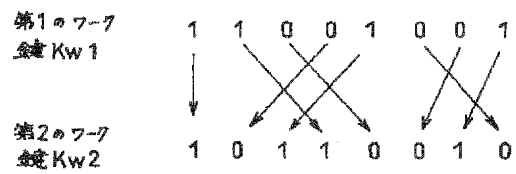
【図3】



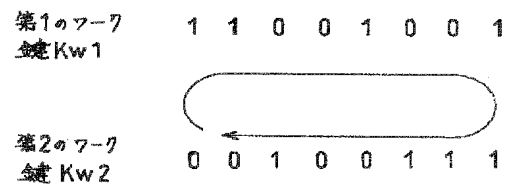
【図1】



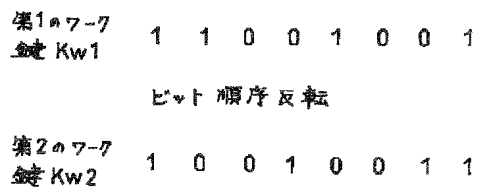
【図4】



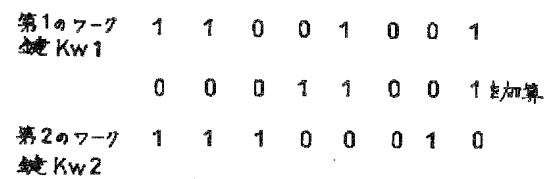
【図5】



【図6】



【図7】



【図8】

